



DEPARTMENT OF THE NAVY

NAVAL SEA SYSTEMS COMMAND, WASHINGTON NAVY YARD, DC 20376-4065
NAVAL AIR SYSTEMS COMMAND, PATUXENT RIVER, MD 20670-1547
NAVAL SUPPLY SYSTEMS COMMAND, MECHANICSBURG, PA 17055-0791
NAVAL FACILITIES ENGINEERING COMMEAND, WASHINGTON NAVY YARD, DC 20374-5065
SPACE AND NAVAL WARFARE SYSTEMS COMMAND, SAN DIEGO, CA 92110-3127
MARINE CORPS SYSTEMS COMMAND, QUANTICO, VA 22134-6050

MARCORSYSCOM Order	SPAWARINST 3058.1	NAVFACINST 5000.15
5000.3 MCSC 06	SPW 05A	FAC CI
6 Jun 2008	7 Apr 2008	6 Mar 2008

NAVSUPINST 5000.20	NAVAIRINST 5000.21B	NAVSEAINST 5000.8
SUP 31	AIR-4.1	Ser TAB/032
10 Jun 2008	24 Jan 2008	21 Jul 2008

From: Commander, Naval Sea Systems Command
Commander, Naval Air Systems Command
Commander, Naval Supply Systems Command
Commander, Naval Facilities Engineering Command
Commander, Space and Naval Warfare Systems Command
Commander, Marine Corps Systems Command

Subj: NAVAL SYSCOM RISK MANAGEMENT POLICY

Ref:

- (a) SECNAVINST 5400.15C, Department of the Navy (DON) Research and Development, Acquisition, Associated Life Cycle Management, and Logistics Responsibilities and Accountability, of 13 Sep 2007
- (b) VS-JI-22A, Virtual SYSCOM Engineering and Technical Authority Policy, of 31 Jan 2007
- (c) DOD Directive 5000.1, The Defense Acquisition System, of 12 May 2003
- (d) DOD Instruction 5000.2, Operation of the Defense Acquisition System, of 12 May 2003
- (e) DOD Instruction 6055.7, Accident Investigation, Reporting and Record Keeping, of 3 Oct 2000
- (f) USD Memorandum, Defense Acquisition System Safety - ESOH Risk Acceptance, of 7 Mar 2007
- (g) SECNAVINST 5000.2C, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, of 19 Nov 2004
- (h) MIL-STD-882D, Standard Practice for System Safety, of 10 Feb 2000
- (i) OPNAVINST 5100.24B, Navy System Safety Program Policy, of 6 Feb 2007
- (j) OPNAVINST 8020.14/Marine Corps Order P8020.11, Department of the Navy Explosives Safety Policy, of 1 Oct 1999
- (k) NAVSEAINST 8020.6E, Department of the Navy Weapon Systems Explosives Safety Review Board, of 11 Mar 2008

DISTRIBUTION STATEMENT A: Approved for Public Release;
Distribution is Unlimited.

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

- (l) Risk Management Guide for DOD Acquisition, Sixth Edition, Version 1.0, of August 2006
- (m) MARCORSYSCOM ESOH Handbook of 5 Jan 06

Encl: (1) NAVAL Program Risk Reporting Matrix
 (2) Excerpts from MIL-STD-882D
 (3) System Safety Risk Matrices

1. Purpose. To establish policy and assign responsibilities for a standardized risk management process across all Naval Systems Commands (SYSCOMs) and affiliated Program Executive Officers (PEOs), consistent with references (a) through (l).

2. Cancellation. This instruction supersedes NAVAIRINST 5000.21A.

3. Scope and Applicability. This instruction applies to all Naval SYSCOMs and their affiliated PEOs, consistent with the scope of references (a) and (b) and within the implementation of references (c) through (m). This instruction does not apply to Operational Risk Management per OPNAV Instruction 3500.39B, or to the exclusions listed in reference (b), which includes all matters under the cognizance of the Naval Nuclear Propulsion Directorate (SEA 08). Application of this instruction shall be consistent with reference (d) Defense Acquisition System Policies, including Flexibility, Responsiveness, Innovation, Discipline, and Streamlined and Effective Management.

4. Discussion

a. Definition of Risk. Risk is the potential for mishaps or other adverse variation in the cost, schedule or performance of a program or its products. Reference (h) defines a System safety mishap as unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. While such variation can include positive opportunities, risk is more generally considered to be the potential for a negative future reality. A description of risk is in future terms that help identify both possible future effects and the root cause(s). Risk is classified into program risk (high, moderate, low) based on likelihood and consequence, or system safety risk (high, serious, medium, low) based on probability or frequency of occurrence, and severity.

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

b. Definition of Risk Management. Risk management is an organized method for continuously identifying and measuring risk; developing mitigation options; selecting, planning, and implementing the appropriate risk mitigations; and accepting and tracking risks when it is no longer prudent to further mitigate them. Risk management is a process that evaluates the likelihood or probability of an undesirable event occurring; assesses the consequences or severity of the event should it occur; evaluates the sources or root causes of the risk; and identifies the available risk mitigations.

(1) An effective risk management process is evidenced by early identification and analysis of risks, planning to mitigate those risks, early implementation of corrective actions, continuous tracking and reassessment. An effective risk management process depends on effective awareness training, open communication, concise documentation, and close coordination between programmatic and technical authorities, consistent with reference (b). Programmatic authorities include Milestone Decision Authorities (MDAs), the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN RD&A), Program Executive Officers (PEOs) and Program Manager (PMs). Technical authorities include the SYSCOM Commanders, SYSCOM Chief Engineers, Deputy Warranting Officers (DWOs) and Technical Warrant Holders (TWHs).

(2) Risk management efforts include a complete review of all areas required to support the life cycle of a given system. Risk areas or sources can include requirements, research, design, development, hardware, software, interfaces, systems engineering, interoperability and integration, production transition, test and evaluation (T&E), system safety, human performance capability, manpower and Sailor training, funding, logistics elements, engineering support, readiness, environmental impact, contracts, management, staffing work years, process, disposal, and other risk sources such as those listed in references (h), (l) and (m).

(3) As a program matures through its life cycle, the type and character of risks will change. References (c) and (d) describe management principles and policies applicable to all Department of Defense (DOD) acquisition programs, and require Program Managers (PMs) and other acquisition managers to continually assess and reduce risks.

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

(4) References (c) and (d) define the DOD acquisition process for all programs and require that systems engineering principles permeate the design, manufacture, T&E, and product support of DOD acquisition programs. In a systems engineering environment, risk management is an essential and integral part of technical program management throughout the life cycle.

(5) As a program transitions through developmental and operational testing and then to Fleet use, Risk Management Plans (RMPs) are structured to identify, assess, and mitigate risks that have a risk impact on safety or the overall program's cost, schedule, and/or performance. RMPs need to define the overall program approach to capture and manage risks.

(6) References (f) through (k) define DON policy for system safety and for naval weapons and explosive safety that programs are required to follow. Reference (m) provides information and resources for the execution of system safety for USMC program management teams. Reference (h) contains several tools to assist in performing system safety risk analysis. It should be noted that an RMP and process does not suffice for a complete system safety program. System safety involves many other activities in addition to a hazard-mishap risk management process, as discussed in references (i) and (m). Safety hazard risk planning is contained in the System Safety Program Plan (SSPP) required by reference (h).

c. Definition of Residual Risk. Residual risk is the risk that remains after mitigation. Risk mitigation will often lower the risk, or even eliminate the risk. Formal acceptance of risk is normally described as the acceptance of residual risk, as stated in this instruction.

d. Additional Guidance. The DOD Risk Management Guide, reference (l), is a supplemental publication that provides guidance and procedures for conducting program risk assessments and developing RMPs. This document is accessible in the Defense Acquisition University on line library at www.acq.osd.mil/se/publications.htm.

5. Policy. To ensure compliance with the risk management requirements of references (c) through (k), all acquisition and in-service programs shall establish, maintain and utilize an

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

integrated risk management process. Risk Management Boards (RMBs) and RMPs are components of the risk management process. Programmatic and technical authorities are both essential to an effective risk management process and shall be integral participants. Risk management shall be accomplished using the fundamental steps listed below and tailored consistent with reference (c). Reference (c) directs that there is no one best way to structure an acquisition program to accomplish the objective of the Defense Acquisition System. Milestone Decision Authorities (MDAs) and PMs shall tailor program strategies and oversight, including documentation of program information, acquisition phases, the timing and scope of decision reviews, and decision levels, to fit the particular condition of that program, consistent with applicable laws and regulations and the time-sensitivity of the capability need.

a. Risk Identification. Efforts shall be applied to identify risks early enough in the lifecycle to allow cost effective risk mitigation efforts. In-service experience (e.g., safety mishap reports, lessons learned, other reference (i) data) from comparable predecessor systems should be reviewed early on to identify potential risks. Individuals throughout the program (Government, industry and the Fleet) shall be encouraged and provided the wherewithal to submit prospective risks for consideration that they feel could adversely impact successful execution of the program or safe and effective operation and support of the eventually fielded system. Risk identification shall not be limited to risk associated with the particular program; it shall include cross-program risks and risks that the program may be generating for other programs.

b. Risk Analysis and Assessment. Technical authorities shall provide independent technical risk analysis for the identified risks, including determination of the level of risk, to programmatic authorities. Programmatic authorities will then factor those analyses into the program risk assessment, which also includes cost and schedule variables. Risk analysis and assessment should address compound risks such as several small risks becoming a larger risk, and cross-program risks within DON and Cross-Service.

c. Risk Mitigation Planning. Programmatic authorities shall mitigate risks in a manner that balances risk with cost, schedule and performance constraints and ensures mishap risk is mitigated to an acceptable level. Cost impacts shall be addressed from a

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

lifecycle perspective, including operations and support costs along with acquisition cost. Technical authorities shall assist the programmatic authorities by developing and evaluating risk mitigation options and participating in risk mitigation efforts. As stated in reference (b), technical authorities identify and evaluate technical alternatives, determine which are technically acceptable, and perform associated risk and value assessments of those alternatives. For system safety risk mitigation, reference (h) outlines a preferred order of precedence for mitigation, which should be contained in the planning guidelines and process. This order of precedence is very important in properly mitigating the safety risk presented by hazards.

d. Risk Mitigation Plan Implementation. Programmatic authorities shall adequately resource risk mitigation efforts to ensure the effectiveness of those efforts.

e. Risk Retirement. Risk retirement occurs when risk mitigation efforts have succeeded such that it would no longer be identified as a risk. Retired risks do not need further tracking.

f. Risk Tracking. Programmatic and technical authorities shall track risks using the standard matrices for evaluating and reporting both program risks (depicted in enclosure (1)), and system safety risks (depicted in enclosures (2) and (3)). For residual risks that have been accepted, the RMP shall describe any associated monitoring and data. When a program transitions from acquisition to in-service, the RMP shall be delivered to the in-service program manager who shall continue to manage it.

(1) Program Risks. The Program Risk Matrix depicted in enclosure (1) uses standard likelihood and consequence definitions to plot specific risks. The plotted position shows the current assessment of the risk's likelihood and the estimated consequences of its effect on the program when the risk manifests. As risk mitigation succeeds, a high or moderate risk's position will migrate in successive assessments from its current location toward low risk, or be completely eliminated.

(2) System Safety Risks. The management of a program's system safety process shall be in accordance with references (f) and (g), which require using reference (h) and the techniques described in Tables A-I through A-IV therein. Page one of enclosure (3) depicts the MIL-STD-882D (reference (h)) System

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

Safety Risk Matrix that plots probability or frequency against severity. Page two of enclosure (3) shows a tailored system safety risk matrix which meets a specific community of systems (NAVAIR) needs. All system safety risks shall be included in the Program's System Safety Risk Matrix. This includes program risks that also have a system safety aspect and system safety risks that may be created through the mitigation of program risks. Similarly, systems safety risks that will have impact on cost, schedule or performance shall be integrated into the overall program risk management structure.

(3) Risk Descriptions. Each risk description shall include three key elements:

- (a) A brief description of the risk;
- (b) A brief description of the root causal factor(s) for the risk and;
- (c) The proposed/planned mitigations that address the source(s) and effect(s).

g. Residual Risk Acceptance. Consistent with references (a) through (k), the appropriate programmatic authority shall formally accept residual risks. As stated in the reference (l) guidance, the status of program risks should be reported to the appropriate PEO/PM/SYSCOM Commander and user personnel prior to Milestone decisions, following significant risk changes, or as requested. As required by reference (g), residual system safety risks, reference (h), shall be accepted prior to exposing people, equipment, or the environment to known system-related ESOH hazards. The level of technical authority approving the analysis of the residual risk shall be equivalent to the level of the programmatic authority accepting the residual risk. The technical authority that approves the analysis of the residual risk shall ensure it has been coordinated with other technical authorities. Technical and programmatic authorities shall coordinate residual risk analysis and acceptance with their Fleet counterparts to ensure alignment with Fleet objectives, especially with respect to risks related to operational capability or operations and support costs. The following table shall be used to identify the appropriate approval levels for analyzing and coordinating the acceptance of residual risk. Additional details needed to define who these individuals are for a particular program shall be contained in the RMP.

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
 NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

RESIDUAL RISK ACCEPTANCE SUMMARY

Level of Risk:	Technical Authority: Approves Analysis of Residual Risk	Programmatic Authority: Accepts Residual Risk	User/Fleet Coordination: (Typical - the RMP shall detail the specific Fleet/User Organizations)	
Program:			Acquisition:	In-Service:
High	SYSCOM COMMANDER	MDA or RDA	OPNAV Nx MCCDC***	Lead TYCOM (Fleet), MCCDC
Moderate	DWO	PEO	OPNAV Nxy	Lead TYCOM (Fleet)
Low	TWH	PM	OPNAV Nxyz	TYCOM N43 or Wing Commander (Fleet)
System Safety:			Acquisition:	In-Service:
High*	SYSCOM COMMANDER	RDA	OPNAV Nx MCCDC	Lead TYCOM (Fleet), MCCDC
Serious*	DWO	PEO	OPNAV Nxy MCCDC	Lead TYCOM (Fleet), MCCDC
Medium	TWH	PM	OPNAV Nxyz	TYCOM N43 or Wing Commander (Fleet)
Low	TWH or Certificate Holder**	PM		

Notes:

- * Formal User/Fleet concurrence is required.
- ** In some cases, the TWH will choose not to delegate this authority to certificate holders, as in the case of explosives safety, which is governed by reference (k).
- *** Marine Corps Combat Development Command (MCCDC)

h. Conflict Resolution. Whenever programmatic and/or technical authorities disagree on a technical issue, such as classifying the level of risk, the conflict resolution policy of reference (b) applies. If it is unclear how a particular risk should be classified, the following or similar approach should be used to resolve the conflict before elevating it as required by reference (b). The participants should mutually determine what level of authority should approve the technical risk analysis and accept the residual risk, and then classify the level commensurate with that understanding.

6. Action. SYSCOMs and affiliated Programmatic Authorities shall implement the policies and requirements contained in this Instruction. The following responsibilities are assigned relative to the risk management process.

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

a. PEOs and SYSCOM Commanders. PEOs and SYSCOM Commanders are responsible for:

(1) Ensuring program acquisition plans and strategies provide for risk management and that identified risks are considered in milestone decisions;

(2) In conjunction with the Head of Contracts, ensuring program contract(s) Statement of Objectives (SOOs), Statements of Work (SOWs) and Contract Deliverable Requirements Lists (CDRLs) include provisions to support a defined risk management plan and process; and

(3) Ensuring each acquisition and in-service program has a defined RMP that addresses both program and system safety risks; and that risk assessments are conducted and risk management performed per that plan. PEOs and SYSCOM Commanders may issue guidance to their PMs on tailoring RMPs to meet unique PEO or SYSCOM needs.

b. PMs. PMs are responsible for:

(1) Establishing, using, maintaining, and funding an integrated risk management process, including all aspects addressed by this instruction. PMs shall ensure their integrated risk management process includes all disciplines required to support the life cycle of their system (e.g., systems safety, logistics, systems engineering, producibility, in-service support, contracts, tests, etc.). If the contract under review is subject to Earned Value Management system criteria, consider any areas of concern identified in the Cost Performance Report, milestone charts, Integrated Master Schedule, or similar systems, which assess contractor performance on the contract;

(2) Forming a program RMB or equivalent that shall include a lead programmatic authority (e.g., the PM or Integrated Program Team (IPT) Leader) and a lead technical authority (i.e., the TWH who is the Chief/Lead Systems Engineer for the program). The RMB may also include the Risk Management Coordinator, Chief Logistician, Budget and Financial Manager (BFM), Cost Analyst, Prime Contractor, and other members relevant to the program strategy, phase, risks and Systems Safety. Consistent with reference (d), MDAs and PMs may tailor or combine RMBs to fit the particular conditions of the program(s);

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

(3) Including Fleet operational users (Type Commanders, Wing Commanders, etc. (referred to as the Fleet) in identification of risks related to the anticipated user population or operational capability and in the formulation and acceptance of risk mitigation plans;

(4) Reporting both program and system safety risks to the PEO, the SYSCOM Commander and Fleet personnel prior to Milestone decisions, following significant risk changes, or as requested; and

(5) Reporting program risk assessments to the Independent Logistics Assessment (ILA) and Initial Operational Capability Supportability Review (IOCSR) teams per reference (c). This will address supportability risk impact on the program equally with other technical, cost and schedule risk consequences.

c. RMBs. RMBs are responsible for overseeing the risk management process for the PM, including oversight of:

(1) RMP Development, maintenance and implementation;

(2) Risk assessments per the RMPs;

(3) Continual assessments of the Program for new risks, the status of existing risks, and management of risk mitigation activities. The RMB's focus should be on ensuring risks that jeopardize the achievement of significant program requirements, thresholds, objectives, or safety are properly identified, analyzed and mitigated;

(4) Development of appropriate risk mitigation strategies for each high or moderate program risk and each high, serious or medium system safety risk, including estimation of funding requirements to implement risk mitigation plans; and

(5) Reporting both program and system safety risks to the appropriate PEO/PM/SYSCOM and Fleet personnel.

d. IPTs. IPTs, or equivalent bodies as defined in the RMP, assist the PM in managing the program and the design and configuration of naval products. Regarding risk management, IPTs are responsible for:

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

(1) Supporting the RMB, including assisting in writing, maintaining and implementing the RMP;

(2) Assessing risks using enclosures (1), (2), and (3), and consulting the DOD Risk Management Guide and the Standard Practice for System Safety, references (l) and (h). Ongoing or continual risk assessments are highly recommended, and are useful during all phases of a program's life cycle. Tailored program and safety risk assessments shall be conducted for each of the applicable systems engineering technical reviews (SETRs) and for each key program decision point;

(3) Recommending appropriate risk mitigation strategies for each high and moderate program risk and for each high, serious and medium system safety risk, including estimating funding requirements to implement risk mitigation plans. Providing risk mitigation support when required. Implementing and obtaining Fleet acceptance of risk mitigation in accordance with program guidance from the RMB per the program RMP; and

(4) Reporting on both program and system safety risks to the RMB.

e. Technical Authorities. Technical Authorities are responsible for:

(1) Providing the trained people and processes to support the technical aspects of risk management;

(2) Designating TWHs and Certificate Holders (CHs) in accordance with reference (b) and making them available to assist with risk management activities;

(3) Providing personnel to conduct independent risk assessments on specific programs upon request of PMs or higher authority; and

(4) Performing technical risk identification and analysis within their reference (b) technical domains, and participating in the risk management process as detailed in this instruction.

7. Review. The Naval SYSCOM Systems Engineering Stakeholders Group (SESG) shall review this instruction annually, coordinating and implementing updates and changes as appropriate.

MARCORSYSCOM 5000.3 SPAWARINST 3058.1 NAVFACINST 5000.15
NAVSUPINST 5000.20 NAVAIRINST 5000.21B NAVSEAINST 5000.8

Distribution:

SNDL FKP COMNAVSEASYSYSCOM Shore Activities
C84 COMNAVSEASYSYSCOM Shore Based Detachments
NAVSEA Special List Y1
A1J1F PEO SHIP
A1J1L PEO IWS
A1JIM PEO LMW
AIJIN PEO SUB
AIJ1Q PEO CARRIERS
21A1 CFFC
21A2 COMPACFLT
24A Air Force Commanders
24D Surface Force Commanders
24G Submarine Force Commanders
26U Regional Maintenance Centers
FT88 EDOSCOL
DRPM ERP
FKA1C COMNAVFACENGCOM
AIR 1.0, 4.0, 5.0 and 6.0
PEO (T)
PEO (A)
PEO (W)
NAWC AD, WD
FKQ SPAWAR Activities
SPAWAR 00, 01, 02, 04, 05, WLA
NETWARCOM
SPAWAR ITC (00)
PEO C4I AND SPACE
PEO IT
PEO SPACE SYSTEMS
DRPM NMCI
MARCORSYSCOM Deputy for C4I Integration
MCCDC
NAVSAFCECEN, Naval Safety Center
RDA CHSENG

NAVAIRHQs Directives Web Address:

<http://directives.navair.navy.mil> or

<https://mynavair.navair.navy.mil/portal/server.pt>

NAVSUP (Electronic only via the Naval Logistics Library (NLL))

Web site <https://nll.ahf.nmci.navy.mil>)

NAVAL Program Risk Reporting Matrix

1. Each undesirable event that might affect the success of the program (technical, schedule, and cost) will be identified and assessed as to likelihood and consequence of occurrence.

2. A standard format for evaluation and reporting of program risk assessment findings will facilitate common understanding of program risks at all levels of the organization. The matrix below will be used to determine the level of risks identified within a program. The level of risk will be reported as low, moderate, and high represented in the matrix with the colors green-low, yellow-moderate, and red-high.

Likelihood	Level	Likelihood	Probability of Occurrence
	1	Not Likely	~10%
	2	Low Likelihood	~30%
	3	Likely	~50%
	4	Highly Likely	~70%
	5	Near Certainty	~90%

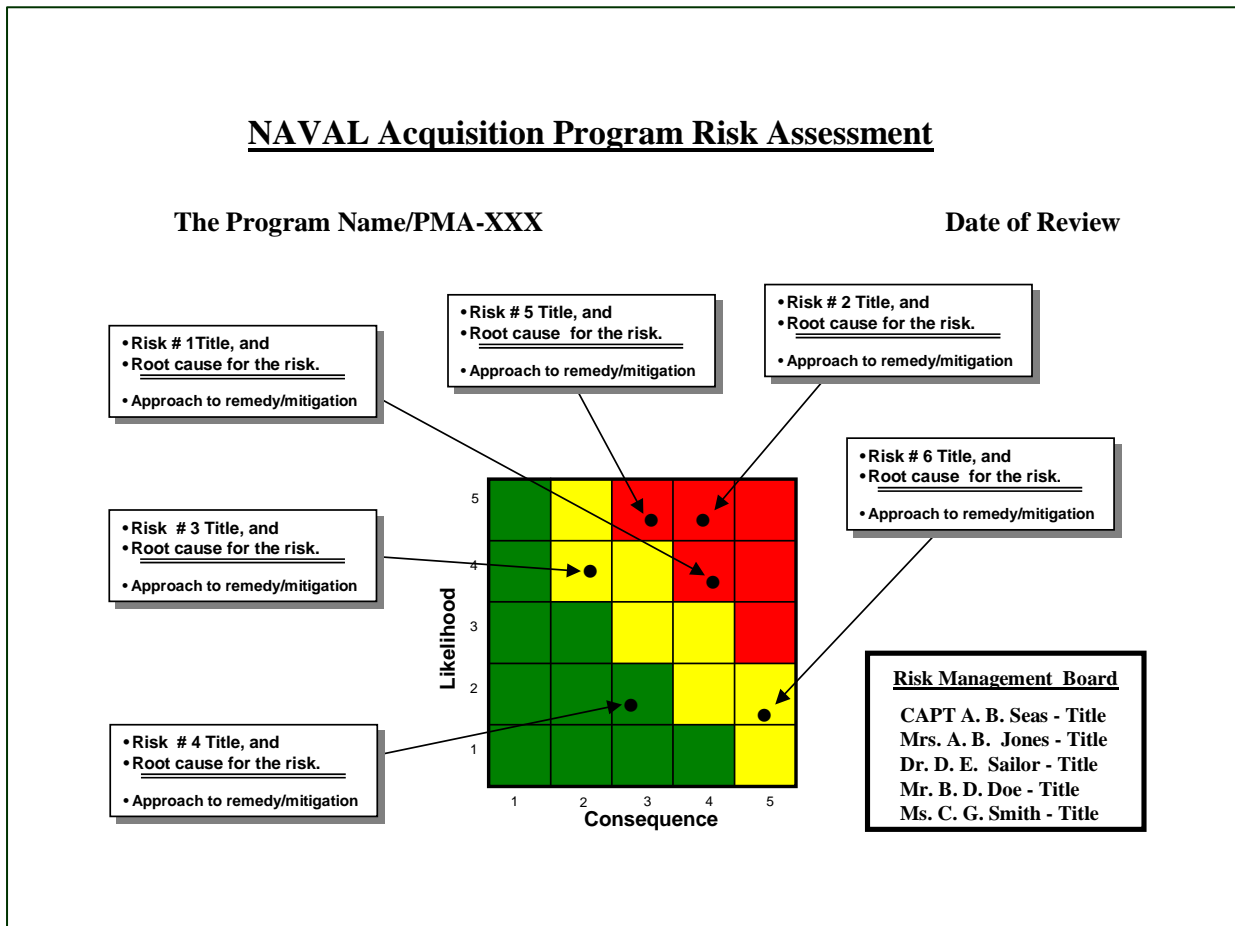
Likelihood	5					
	4					
	3					
	2					
	1					
		1	2	3	4	5

Consequence	Level	Technical Performance	Schedule	Cost
	1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
	2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program; same approach retained	Additional activities required, able to meet key dates. Slip < * month(s)	Budget increase or unit production cost increases < ** (1% of Budget)
	3	Moderate reduction in technical performance or supportability with limited impact on program objectives; workarounds available	Minor schedule slip, no impact to key milestones. Slip < * month(s) plus available float of critical path. Sub-system slip > * month(s) plus available float.	Budget increase or unit production cost increase < ** (5% of Budget)
	4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success; workarounds may not be available or may have negative consequences	Program critical path affected, all schedule float associated with key milestone exhausted Slip < * months	Budget increase or unit production cost increase < ** (10% of Budget)
	5	Severe degradation in technical performance; Cannot meet KPP or Key technical/supportability threshold; will jeopardize program success; no workarounds available	Cannot meet key program milestones Slip > * months	Exceeds Acquisition Program Baseline (APB) threshold > ** (10% of Budget)

* - Tailor for program in month(s)
** - Tailor for program in whole dollars

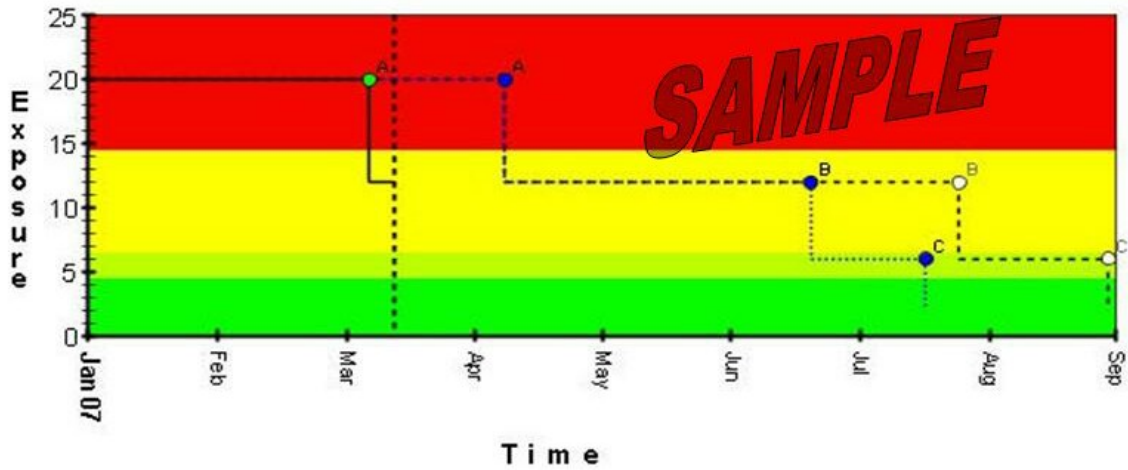
Briefing Format

- Below is an example of the format that will be used when reporting the results of a program risk assessment.
- Presenter should be prepared for more detailed discussions on these issues and alternative mitigation plans.
- List the members and their affiliation if a standing advisory board does the assessment formally.
- The 5x5 matrix and color scheme shall remain common with this enclosure unless otherwise authorized by the cognizant SYSCOM Commander.



5. Risk mitigation is often displayed in a waterfall chart to show the reduction and expected reduction in risk exposure as mitigation actions are completed over time. A sample waterfall chart from the Naval Systems Engineering Resource Center (NSERC) risk exchange tool is shown below:

Waterfall Chart



<https://nserc.navy.mil>

Excerpts from MIL-STD-882D

A.4.4.3.2.1 Mishap severity. Mishap severity categories are defined to provide a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. Suggested mishap severity categories are shown in Table A-I. The dollar values shown in this table should be established on a system by system basis depending on the size of the system being considered to reflect the level of concern.

TABLE A-I. Suggested mishap severity categories.

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding \$1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding \$200K but less than \$1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding \$10K but less than \$200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding \$2K but less than \$10K, or minimal environmental damage not violating law or regulation.

NOTE: These mishap severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the program manager and the developer as to the meaning of the terms used in the category definitions. Other risk assessment techniques may be used provided that the user approves them.

A.4.4.3.2.2 Mishap probability. Mishap probability is the probability that a mishap will occur during the planned life expectancy of the system. It can be described in terms of potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative mishap probability to a potential design or procedural hazard is generally not possible early in the design process. At that stage, a qualitative mishap probability may be

derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability is documented in hazard analysis reports. Suggested qualitative mishap probability levels are shown in Table A-II.

TABLE A-II. Suggested mishap probability levels.

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

*Definitions of descriptive words may have to be modified based on quantity of items involved.

**The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

A.4.4.3.2.3 Mishap risk assessment. Mishap risk classification by mishap severity and mishap probability can be performed by using a mishap risk assessment matrix. This assessment allows one to assign a mishap risk assessment value to a hazard based on its mishap severity and its mishap probability. This value is then often used to rank different hazards as to their associated mishap risks. An example of a mishap risk assessment matrix is shown at Table A-III.

TABLE A-III. Example mishap risk assessment values.

SEVERITY	Catastrophic	Critical	Marginal	Negligible
PROBABILITY				
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

A.4.4.3.2.4 Mishap risk categories. Mishap risk assessment values are often used in grouping individual hazards into mishap risk categories. Mishap risk categories are then used to generate specific action such as mandatory reporting of certain hazards to management for action or formal acceptance of the associated mishap risk. Table A-IV includes an example listing of mishap risk categories and the associated assessment values. In the example, the system management has determined that mishap risk assessment values 1 through 5 constitute “High” risk while values 6 through 9 constitute “Serious” risk.

TABLE A-IV. Example mishap risk categories and mishap risk acceptance levels.

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

*Representative mishap risk acceptance levels are shown in the above table. Mishap risk acceptance is discussed in paragraph A.4.4.7. The using organization must be consulted by the corresponding levels of program management prior to mishap risk acceptance.

System Safety Risk Matrices

This enclosure contains two system safety risk matrices. The first is a direct application of the MIL-STD-882D system safety risk matrix. The second is a system safety risk matrix tailored to meet the needs of NAVAIR.

MISHAP PROBABILITY	MISHAP SEVERITY			
	Catastrophic (I)	Critical (II)	Marginal (III)	Negligible (IV)
Frequent (A)	HIGH	HIGH	SERIOUS	MEDIUM
Probable (B)	HIGH	HIGH	SERIOUS	MEDIUM
Occasional (C)	HIGH	SERIOUS	MEDIUM	LOW
Remote (D)	SERIOUS	MEDIUM	MEDIUM	LOW
Improbable (E)	MEDIUM	MEDIUM	MEDIUM	LOW

NAVAIR SYSTEM SAFETY RISK MATRIX

HAZARD CATEGORIZATION		S E V E R I T Y			
		CATASTROPHIC (1)	CRITICAL (2)	MARGINAL (3)	NEGLIGIBLE (4)
F R E Q U E N C Y	FREQUENT (A) = or > 100/100K flt hrs	1	3	7	13
	PROBABLE (B) 10-99/100K flt hrs	2	5	9	16
	OCCASIONAL (C) 1.0-9.9/100K flt hrs	4	6	11	18
	REMOTE (D) 0.1-0.99/100K flt hrs	8	10	14	19
	IMPROBABLE (E) = or < 0.1/100K flt hrs	12	15	17	20

UNACCEPTABLE

ASN/CNO / CMC/CFFC*
 Acceptance
 1-5 HIGH SAFETY RISK

**ACCEPTABLE
 WITH REVIEW**

PM/TYCOM N43/WING CDR* Acceptance
 11-17 MEDIUM SAFETY RISK

UNDESIRABLE

PEO/CFFC N43/TYCOM*
 Acceptance
 6-10 SERIOUS SAFETY RISK

**ACCEPTABLE
 WITHOUT REVIEW**

PM/RMB Acceptance
 18-20 LOW SAFETY RISK

* Fleet Acceptance for aircraft that have achieved IOC

Severity is the worst credible consequence of a hazard in terms of degree of injury, property damage or effect on mission defined below:

Catastrophic - Class A (damage > \$1M / fatality / permanent total disability)

Critical - Class B (\$200K < damage < \$1M / permanent partial disability / hospitalization of 3 or more personnel)

Marginal - Class C (\$20K < damage < \$200K / injury results in 1 or more lost workdays)

Negligible - All other injury/damage less than Class C

Probability of occurrence for discrete events may replace **Frequency** based upon the chart below:

